AFFIDAVIT OF ROBERT ERDELY

1. I have 25 total years of experience in law enforcement. For over18 years I specialized in computer crime, and for 12 years, and at the present time, I provided instruction to law enforcement officers on the skills necessary to conduct online investigations and computer forensic examinations, including investigations involving peer-to-peer file sharing networks. Attached to this affidavit as Exhibit 1 is a true and accurate copy of my CV.

2. I am currently a Detective with the Computer Crime Unit of the Indiana County Pennsylvania's Detective Bureau. I was previously employed as the supervisor for the Pennsylvania State Police Computer Crime Unit until I retired in 2012. Both Computer Crime Units are responsible for investigations of crimes which occur on the Internet including the distribution of child exploitation material through peer-to-peer networks.

3. With one other individual, I created the ICAC law enforcement system that law enforcement organizations use to identify potential possessors and distributors of child pornography over the BitTorrent peer-to-peer (P2P) sharing network. I am thus intimately familiar with the creation of this system, the use of the system, and the technical specifications and capabilities of the system. I conduct trainings for law enforcement officers on how to utilize the ICAC law enforcement system. The investigation in this case involved the BitTorrent P2P sharing network.

4. In laypersons' terms, the ICAC law enforcement system identifies potential sharers of child pornography in essentially the same way that any other individual P2P user seeking to share child pornography identifies a potential source of that child pornography.

5. P2P networks first gained notoriety in the music file sharing context with programs such as Napster and Limewire. The main difference between other P2P networks and BitTorrent is that BitTorrent does not provide a search engine to locate files being shared on the BitTorrent network.

6. Instead, to receive or distribute child pornography over the BitTorrent P2P network, a defendant must first obtain a "torrent file" from an outside website or some other source of that data. A torrent file does not contain the actual file itself (in this case, the actual child pornography image). It only contains information about the file(s), such as the name, size, folder structure, and cryptographic

CARDELS 800-783-0399
GOVERNMENT
EXHIBIT
2

"hash value" (Sha-1) for the data of the file(s) being shared. The torrent file also contains information about where the user can learn how to obtain the file itself.

7. Hash values are an alpha/numerical identifier for a given file, and certain hash values can identify a given file as child pornography. The Secure Hash Algorithm (SHA-1) was developed by the National Institute of standards and Technology (NIST), along with the National Security Agency (NSA). The BitTorrent file sharing network uses this hashing algorithm to identify the files being shared on this network. The odds of the Sha-1 hashing failing (i.e. - two different files producing the same Sha-1 hash) is 2^{160}, or 1 in 1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000,000.

8. These BitTorrent indices are essentially matchmakers. More specifically, they are computers or servers that identify and match people using BitTorrent with other people using BitTorrent who are looking for or are actively sharing the same file(s) described by the .torrent file. Those matches are called "download candidates." BitTorrent indices typically match multiple download candidates with each other. The BitTorrent program can then connect to 1 or many download candidates and request to download the pieces of the files needed. That process is often referred to as "swarming." Both the sharing computer and the downloading computer must have the same torrent file (identified through a unique identifier called an "infohash"). Without having the same .torrent file, downloading a file or files is impossible. This is easily confirmed by anyone by reading the well documented BitTorrent protocol.

9. After the defendant loads a .torrent file into his/her BitTorrent application, the BitTorrent program will initiate contact with BitTorrent index to locate download candidates. A defendant, through his computer and BitTorrent program, provides the BitTorrent index with certain information, including the defendant computer's IP address and the unique identifier of the .torrent, which contains the instructions on how to download the file(s) that the defendant is seeking to download and/or share. The infohash is based on the Sha-1 algorithm and therefore is a very reliable way to uniquely identify every collection of file(s) being shared on the BitTorrent file sharing network.

10. A BitTorrent index does not initiate contact with a defendant or "request" information from a defendant's computer. To the contrary, a defendant, through his computer, voluntarily contacts the BitTorrent index and voluntarily provides the BitTorrent index with the defendant's IP address and the infohash of the data that the defendant is seeking to download or share. In fact, a defendant shares

that information with the BitTorrent index for the very purpose of the BitTorrent index, in turn, sharing that information with other potentially unknown peers who possess, or are seeking the same file.

11. There are a few very minor differences between the ICAC law enforcement system's use of the BitTorrent P2P system and a "peer's" use of the P2P system. With respect to the first difference, as previously stated, ordinary defendants/BitTorrent users must obtain a .torrent file before they can seek a given file from another peer through a BitTorrent network. The ICAC law enforcement system, however, maintains those .torrent files and hash values, so the ICAC investigators does not have to search outside websites for that information.

12. The second minor difference relates to the actual P2P download. Law enforcement uses software to engage in a single-source download from a solitary download candidate. This is an example of Law Enforcement being more restrictive than the original design of BitTorrent which seeks to download from many sharing computers to speed up the download times. This software was not built on any existing software but instead was created for Law Enforcement through a partnership with a University in Massachusetts.

13. The third difference is that the law enforcement software does not share any of the content downloaded during an investigation.

14. If the source code or certain other details about the ICAC system became public, child pornography distributors could find a way to avoid detection from the ICAC system and could render that tool of law enforcement ineffective. Additionally, the .torrent's and the hash values of the files being investigated could hinder future investigations once this identifier to the illegal files became public. The infohash becoming public would also allow others to quickly find and download these child pornography files.

15. I have reviewed the defense expert's declaration where she details how she did not perform any forensic examination but instead relied on the Governments forensic analysis. In paragraph 12 of the defense expert's declaration she states "The report is silent with regard to locating the uTorrent software version 2.2.1" After a review of this case, the defense expert is mistaken in that there was evidence recovered indicating the uTorrent had been installed on a computer seized (reference page 30 of the original forensic report). She later states "Further, the majority of the suspect child pornography was located within system

locations on the hard drive, compressed backup files, external devices, and possibly encrypted containers, so it is unknown if any of those locations would have been publicly available." It is important to note the following regarding most BitTorrent programs, and all of these facts are true regarding uTorrent:

- By default there is no "default download" folder, a user would have to configure this "default download" folder. Even if a "default download" directory was specified, when a torrent file is loaded into uTorrent, a user could save the content to another location, even external hard drives, encrypted drives or network attached storage devices. Each and every location where a user downloads file(s) therefore becomes "publicly shared" whether or not that folder is the users "default download" folder.

- Even though files were found on the external hard drive, even if this was not the default location where they were shared from, any user can move files from location to location. Through my hundreds of investigations, I have learned that it is common for users downloading child pornography to copy and / or move files from location to location, often deleting the file from the original location.

16. BitTorrent performs the sharing of files by downloading "pieces". These pieces downloaded are not typically the whole file but instead a piece of one file or several files. The torrent files are the instructions to download, which includes the sha-1 hash values of each piece. This is used to verify that the piece downloaded from a sharing computer had properly downloaded. The downloaded piece has the sha-1 hash value calculated and then compared to the value located in the torrent file. If the values match, the BitTorrent program knows the download of that piece was successful. This process is used by all BitTorrent programs and this is why it would be **absolutely impossible** to randomly download files from a suspect's computer which are from "unshared folders". Without a torrent file (the instructions), two BitTorrent programs would not be able to share any files. Any expert knowledgeable of the BitTorrent protocol would come to the same conclusion.

17. The software used to conduct investigations was validated by an independent company which employs computer programmers. This independent validation was performed at the FBI's direction. The company was given the program to run and test as well as the source code for review. The following are points of the validation as it relates to the law enforcement bittorrent software which conducts the investigation:

- Source code review
- That the software contacts and downloads from the internet protocol (IP) address and port specified
- That the software properly conducts what is referred to a "single source download" or in other words, the software will only ever download from the one IP address specified.
- That the software is incapable of sharing the downloaded content out to other bittorrent users.
- That the software accurately places the downloaded content into the evidence folder created for each and every investigation.

18. The conclusion of the independent validation was that it passed all operational/validation tests. The program was found to contain a minor bug involving long file paths which was immediately fixed. This minor bug was simply that if a file path became too long, the program would stop performing investigations (i.e. the program would shut down if it encountered a file path which was longer than what Windows allows). This is not at issue since it was fixed.

19. In summary, the ICAC law enforcement system never obtains any unshared information from any computer running a BitTorrent program. If the Law Enforcement tool had the ability to download files other than ones being shared to the BitTorrent network, the independent validation would have revealed it. Additionally, the BitTorrent protocol describes the manner in which this sharing occurs; making the downloading of other material not related to the .torrent file directions an impossibility.

20. Moreover, the ICAC law enforcement system "searches" for download candidates in same way that any public user of the P2P file sharing system "searches" for download candidates. These indexes searched are not the sharing computer, but instead the indexes are the publicly available ones.

21. The ICAC law enforcement system only "searches" for information that a user has already made public by the very use of the uTorrent program. In fact, not only has a defendant's BitTorrent program already provided that information, but the information was provided for the express purpose of sharing that information with other unknown BitTorrent users.

22. BitTorrent by default shares downloaded data back to other BitTorrent users from whatever location the data was saved to, which would include an external hard

drive. The data will continue to be shared as long as the BitTorrent program is running, the computer is connected to the internet, and the .torrent and data remain in the location where they had been downloaded to and the BitTorrent user had not taken an affirmative step to stop sharing that particular .torrent.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge and belief.

Detective Robert W Erdely